Speeding up the Grover algorithm using auxiliary solutions

A.Y. Shiekh*
Diné College, Tsaile, Arizona, U.S.A.

Abstract

It may be possible to extend the Grover search algorithm by taking a divide and conquer approach using auxiliary solutions to achieve an exponential speed-up.

"*What is proved by impossibility proofs is lack of imagination*"
John Bell

1 Introduction

To date there is only one generic search algorithm for quantum computers [1], namely the Grover algorithm, and that achieves a quadratic speed-up over a classical computer.

It is noted here, that the Grover approach is particularly efficient if one quarter of the candidate solutions are valid, and a proposal is made to try and take advantage of this observation by adding auxiliary solutions.

2 Grover's algorithm reviewed

For the sake of illustration we look at the n bit case. Starting with $|0\rangle$ one applies the Hadamard transformation to get the usual spread of $(N = 2^n)$ candidate solutions

$$\left(|0\rangle + |1\rangle + \cdots + |N-1\rangle\right)/\sqrt{N} \tag{1}$$

*shiekh@dinecollege.edu

$|0\rangle$ will have a rather special role to play in this approach, and unlike the others, does not represent a candidate solution[1].

One then applies the Grover four step procedure (to be repeated as many times as necessary)

- Mark the M valid solution(s) (represented by $|\mathbf{S_n}\rangle$) with a π phase change (which is unitary and so allowed). The resultant state is given by:

$$\left(\begin{array}{ccccccc} |0\rangle + |1\rangle + \cdots + & +|\mathbf{S_1}\rangle & + \cdots & +|\mathbf{S_M}\rangle & + \cdots + |N-1\rangle \\ & -2|\mathbf{S_1}\rangle & + \cdots & -2|\mathbf{S_M}\rangle & \end{array} \right) /\sqrt{N} \tag{2}$$

- Perform a Hadamard transformation (H) that will undo the first line to yield:

$$\begin{array}{c} |0\rangle \\ -2\frac{1}{\sqrt{N}} H(|\mathbf{S_1}\rangle + \cdots + |\mathbf{S_M}\rangle) \end{array} \tag{3}$$

- Perform a π phase change on all but the $|0\rangle$ state

$$\begin{array}{c} |0\rangle - 4\frac{M}{N}|0\rangle \\ +2\frac{1}{\sqrt{N}} H(|\mathbf{S_1}\rangle + \cdots + |\mathbf{S_M}\rangle) \end{array} \tag{4}$$

  Crucial to this manipulation is the fact that the Hadamard transform of any candidate begins with $+|0\rangle/\sqrt{N}$.

- Perform another Hadamard transformation that will restore the initial Hadamard spread, but with a reduced amplitude.

$$\begin{array}{ccccc} (1-4\frac{M}{N})(|0\rangle + |1\rangle + \cdots + & |\mathbf{S_1}\rangle + \cdots + |\mathbf{S_M}\rangle & + \cdots + |N-1\rangle)/\sqrt{N} \\ +2(& |\mathbf{S_1}\rangle + \cdots + |\mathbf{S_M}\rangle &)/\sqrt{N} \end{array} \tag{5}$$

What has been achieved is a lowering of the invalid solution amplitudes, and a compensatory lifting of the valid solution amplitudes. In summary, after a single iteration, the probability of finding an invalid solution is given by

$$(N-M)\left(\frac{1-4M/N}{\sqrt{N}}\right)^2 \tag{6}$$

[1] $|0\rangle$ can be separately checked to determine if it is a solution or not, and regardless can be marked as invalid in the processing that follows.

and that of finding a valid solution is

$$M\left(\frac{1-4M/N}{\sqrt{N}}+\frac{2}{\sqrt{N}}\right)^2 \tag{7}$$

and together they indeed sum to unity as they must.

Of particular note is the observation that if one quarter of the candidates are valid, only a single run is needed to eliminate all the invalid solutions, and it is hoped to take advantage of this to speed up the Grover approach.

However, before we do that, it would be good to recover the performance of the standard Grover approach. Begin by defining the normalized sums of valid and invalid solutions: $|\alpha\rangle \equiv (\sum invalid)/\sqrt{N-M}$ and $|\beta\rangle \equiv (\sum valid)/\sqrt{M}$; then the starting state $|\psi\rangle$ is given by

$$|\psi\rangle = \sqrt{\frac{N-M}{N}}\,|\alpha\rangle + \sqrt{\frac{M}{N}}\,|\beta\rangle \tag{8}$$

and the state after one Grover application G is given (from equation 5) by

$$G\,|\psi\rangle = \left(1-4\frac{M}{N}\right)\sqrt{\frac{N-M}{N}}\,|\alpha\rangle + \left(1-4\frac{M}{N}+2\right)\sqrt{\frac{M}{N}}\,|\beta\rangle \tag{9}$$

Re-expressing these in terms of the fraction of valid solutions $f \equiv M/N$, gives these as

$$|\psi\rangle = \sqrt{1-f}\,|\alpha\rangle + \sqrt{f}\,|\beta\rangle \tag{10}$$

$$G\,|\psi\rangle = (1-4f)\sqrt{1-f}\,|\alpha\rangle + (3-4f)\sqrt{f}\,|\beta\rangle \tag{11}$$

Then expressing $\sqrt{f}$ as $\sin\theta/2$ and using the two trigonometric identities $\cos 3\phi = (1-4\sin^2\phi)\cos\phi$ and $\sin 3\phi = (3-4\sin^2\phi)\sin\phi$ simplifies these to

$$|\psi\rangle = \cos\frac{\theta}{2}\,|\alpha\rangle + \sin\frac{\theta}{2}\,|\beta\rangle \tag{12}$$

$$G\,|\psi\rangle = \cos\frac{3\theta}{2}\,|\alpha\rangle + \sin\frac{3\theta}{2}\,|\beta\rangle \tag{13}$$

yielding the picture that each Grover application rotates the state toward the valid solution set by an angle θ given by $\sin\theta/2 = \sqrt{M/N}$; so it takes

the usual Grover approach order $\sqrt{N/M}$ iterations to expose the valid solution set.

Having reviewed the Grover algorithm, we now return to the observation that if one quarter of the solutions are valid, they are isolated in a single iteration of the Grover approach.

3 Divide and conquer mechanism using auxiliary solutions

What is significant about the Grover algorithm is that, up to a point, the more valid solutions that are present the faster it runs, and it is hoped to take advantage of this mechanism by adding (and later removing) auxiliary solutions.

The probability of finding a valid solution after just one iteration is given by equation 7 to be

$$f(3-4f)^2 \tag{14}$$

where $f \equiv M/N$ (the fraction of valid solutions), and as noted before, an optimum is reached when a quarter of the solutions are valid, at which point all invalid solutions are removed in a single iteration of the Grover procedure (see figure 1).

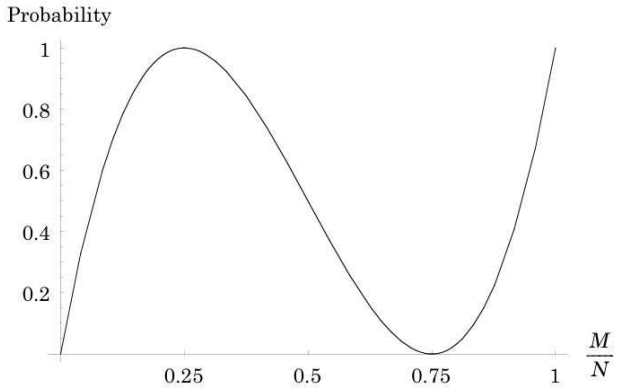

Figure 1: Probability versus fraction of valid solutions

The following supplementary procedure (to be repeated as many times as necessary) is suggested: 'Add' additional auxiliary solutions by considering a candidate solution to be valid not only if it satisfies the criterion to be solved for, but also if the first two bits are each 1. In this way very close to a quarter of the states will be valid[2], and a single run will then eliminate the invalid three quarters.

Having eliminated all invalid solutions not beginning with 11 one would like to repeat the procedure, but only on the remaining quarter.

What one now has (from equation 5) is

$$\frac{1}{\sqrt{M+N_\epsilon}}\left(|\mathbf{S_1}\rangle+\cdots+|\mathbf{S_M}\rangle+\sum|\epsilon\rangle\right) \tag{15}$$

having used $M = N/4$, and where $|\epsilon\rangle$ represents any true solution not beginning with 11 that might have been present in the three quarters that was up for rejection.

Now, $|\mathbf{S_1}\rangle+\cdots+|\mathbf{S_M}\rangle$ is the set of all combinations beginning with 11, so the above may be rewritten as:

$$\frac{1}{\sqrt{M+N_\epsilon}}\left(|11\rangle\left(|0\rangle_{-2}+|1\rangle_{-2}+\cdots+|M-1\rangle_{-2}\right)+\sum|\epsilon\rangle\right) \tag{16}$$

where the new Hadamard spread is now in the space two digits smaller. One might then repeat the Grover approach, using the relevant reduced Hadamard transformation, but not changing the marking function that continues to look at all digits. Each iteration cuts the number of remaining solutions in quarter, so achieving exponential performance.

At completion one will be left with the true solutions as well as the state with all ones, namely $|N-1\rangle$ and this would need to be checked separately, as was also the case for $|0\rangle$, albeit for different reasons.

[2]This could be adjusted to be exactly one quarter if the number of valid solutions were known beforehand.

4 Conclusion

It may be possible to speed up the Grover approach beyond quadratic, by exploiting its somewhat counter-intuitive feature of improved performance, up till the point where one quarter of the solutions are valid. One quarter valid solutions is artificially achieved by temporarily recognizing one in four of the candidate solutions as valid.

Another aspect of this approach is that it uses only the digital aspects of quantum theory for calculation, which might greatly simplify the error correction procedure. The problem with analogue systems is that errors, all be them small, creep into *all* aspects of the system in any finite time, and so are impossible to remove completely. In contrast, digital systems have the advantage that the probability of an error is generally small, albeit that the error itself, if seen, is large; so for a small time interval, it is very unlikely that all aspects of the system find themselves in error.

This proposal gets around the optimality proof as the 'Oracle' changes for each iteration.

References

[1] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, 2000.